

Chat Transcript

Plenary Session WHOIS Changes Under GDPR: Impact to End Users and Public Safety

Wednesday, 21 October 2020 10:30-12:00 CEST

01:04:51 Mary Wong (ICANN org): Hello PANELISTS: Reminder to please speak clearly and at a pace that allows for interpretation. .

01:04:53 hadia Elminiawi: Hello all

01:05:26 Jeffrey Neuman: All - Hello. Can I ask that all of the Questions in the Q&A pod are visible once entered as opposed to only after they are addressed? I am not sure if it is already set up that way, but the past few plenaries, it was not set that way be default. Thanks

01:05:37 Mary Wong (ICANN org): @Jonathan, Panelists: Mark S is not yet here. We will look out for him and add him as a Panelist as soon as we see him.

01:05:48 Cheryl Langdon-Orr: Good evening from Australia

01:05:50 Michele Neylon (Blacknight): +1 Jeff

01:05:54 Maxim Alzoba: hello all

01:05:58 Maxim Alzoba: +1

01:06:08 Jorge Cancio: agree

01:06:08 Svitlana Tkachenko: +1

01:06:14 Jorge Cancio: agree

01:06:22 Svitlana Tkachenko: Hello all from Ukraine!

01:06:23 Elizabeth Behsudi: Hi everyone!

01:06:26 Luc Seufer: Thank you Jeff. For the non native speaker it would be very helpful

01:06:40 Emma CANER: Hello all from France ! :)

01:06:48 Carlos Reyes: @Jonathan, Mark S has not joined yet

01:06:53 hadia Elminiawi: Hello from Egypt

01:07:01 Mary Wong (ICANN org): @Jeff, all - yes I believe we have set the Q&A pod such that all questions asked are visible to all once posted.

01:07:13 Christian Dawson: Thanks Mary

01:07:30 Olevie Kouami / Sénégal: Greetings from Popenguine, Sénégal (West Africa)

01:07:36 Malgorzata Kielar: hello from Poland!

01:07:45 Becky Burr: Hello all

01:07:48 Media Boost: Hi all from Ukraine :)

01:08:03 Jeffrey Neuman: I see that Louie Lee has posted my question so I can see it :)

01:08:10 Louie Lee: Great!

01:08:12 Louie Lee: :)

01:08:34 Hamza Salami Nigeria: Hi everyone from Nigeria

01:08:49 Innocent Adriko: Hi all, greetings from Uganda.

01:08:55 Matthias Pfeifer dot.berlin: hello from Germany

01:09:29 Michele Neylon (Blacknight): Why is the topic "whois"? Whois is dead - everyone has moved to RDAP

01:09:59 Matthias Pfeifer dot.berlin: 'orly?

01:11:00 Olevie Kouami / Sénégal: WHOIS or RDAP ?
01:11:26 Michele Neylon (Blacknight): Well neither really - it should be "domain registration data" or something else
01:11:33 Peter Koch: is this the US regional edition of the panel?
01:11:33 Michele Neylon (Blacknight): but whois is a dead protocol
01:11:37 Luc Seufer: ICANN, one world, one US internet
01:11:41 Michele Neylon (Blacknight): Oh wow ICANN
01:11:42 Lyman Chapin: @Michele we seem to be stuck with "whois" as shorthand for "registration data" indefinitely
01:11:50 Michele Neylon (Blacknight): You're running a GDPR session with a bunch of Americans
01:11:55 Michele Neylon (Blacknight): NOT a single European
01:11:57 Michele Neylon (Blacknight): slow clap
01:12:08 Matthias Pfeifer dot.berlin: :)
01:12:26 Matthias M. Hudobnik: you are right michele ;-)!
01:12:54 Amr Elsadr: @Michele: +1
01:12:55 Jonathan Zuck: @Michele, perhaps we should have been more proactive but the call for interest was not limited to Americans. Those were simply those who showed up for planning the plenary.
01:12:56 Christian Dawson: What a great point, Michele
01:13:08 Matthias M. Hudobnik: you are right michele ;-)!

01:13:11 Pelle wecksell Europol sexual abuse against children: We still need information, but it takes a long time and officers don't know how to contact registrants
01:13:35 Michele Neylon (Blacknight): Jonathan - people don't just "appear" at planning plenaries - they need to be invited
01:13:47 Emma CANER: Totally agree with your Michele..
01:13:48 Jeffrey Neuman: @Jonathan - when a plenary is selected, is there an open call for participants?
01:13:57 Michele Neylon (Blacknight): there are plenty of very well qualified Europeans from all areas of the community that could have spoken to this
01:14:02 Eric Freyssinet: We are in the room (EU/FR law enforcement) here and will ask questions if needed
01:14:11 Michele Neylon (Blacknight): Having an EU law explained to us is hilarious
01:14:15 Mary Wong (ICANN org): @Michele, @Tatiana, all - as Jonathan explained, this session is not about GDPR per se; the panelists will be looking at the present landscape. I'll note also that, as with all other ICANN plenary sessions, these are community-led and community-organized so the topics are selected by the community and the panelists invited by the session organizers.
01:14:25 Olevie Kouami / Sénégal: They could intervene now
01:14:28 Jeffrey Neuman: Perhaps for future plenaries, the topics should be announced and an open call for participants should be announced.
01:14:29 Kristof Tuyteleers: stats please, the public doesn't even know what whois/rdap is
01:14:30 Michele Neylon (Blacknight): The title literally says GDPR

01:14:41 Jonathan Zuck: @Jeff and Michele. Obviously, the panel selection could have gone better. There was an open call for all that were interested in the topic to discuss how it should go.

01:15:04 Olevie Kouami / Sénégal: But its needs an Open Call

01:15:06 Roberto: @Michele - they are not explaining the EU law, they are explaining what they have understood, and that is not necessarily the same thing

01:15:09 Jeffrey Neuman: @Jonathan - I must have missed the open call. Where was it posted?

01:15:11 Volker Greimann: <https://imgflip.com/i/4j9syj>

01:15:18 Michele Neylon (Blacknight): +1 Jeff

01:15:25 Lori Schulman: Gender and Geodiversity continues to be an issue in this space. The panel is very qualified. Nonetheless, Michele and others raise a good point.

01:15:54 Michele Neylon (Blacknight): At least this panel has the gender diversity

01:16:01 Lori Schulman: And those of us who plan, even with the absolute best of intentions, need to be more mindful.

01:16:10 Maxim Alzoba: maybe it should be called US perspective on GDPR implementation in ICANN?

01:16:34 Olevie Kouami / Sénégal: Something is going wrong with this RDAP

01:17:05 Lori Schulman: @Laureen - what is a puppy scam?

01:17:09 Lori Schulman: Free puppies?

01:17:10 Peter Koch: "On the Internet, nobody knows you are a dog"

01:17:15 Lori Schulman: LOL

01:17:29 Matthias Pfeifer dot.berlin: well..aren't we finished with compiling lists of complaints about gdpr?

01:17:29 Mary Wong (ICANN org): All community groups are invited to submit potential plenary topics, and the final list is agreed on by a community-based planning group. The session organizers invite all community groups to participate, via that planning group.

01:18:00 David Taylor: buyapuppy.com is for sale

01:18:04 Luc Seufer: How do you abuse the DNS system to operate a puppy scam?

01:18:29 Maxim Alzoba: if the planning limited to some SGs/ACs - it should be contained in the name of the session then

01:18:42 Olevie Kouami / Sénégal: yesterday was Stats Day

01:18:50 Volker Greimann: thats content. the address should be on the website. make some good content laws, folks

01:18:57 Franck Journoud: Maybe we can attack the substance of the arguments rather than the assumed bias of the speakers?

01:18:58 Mary Wong (ICANN org): @Jonathan - see Michele's question in the Q&A pod; can you type an answer (though I know we have already tried to address it, including in general chat)?

01:19:04 Volker Greimann: europe regulates this well. it works.

01:19:22 Ozan Sahin: @Gabriel - It would be great for the interpreters if you could speak up a bit

01:19:26 Brian King (MarkMonitor): @Franck, you new here? ;-)

01:20:11 Franck Journoud: @Brian: LOL

01:20:13 Maxim Alzoba: there is only local Law Enforcement in the law (if no intergovernmental agreements are in place)

01:20:41 Maxim Alzoba: serving requests from the foreign law enforcement may lead you to a criminal charges

01:21:26 Chris Disspain: you surely don't need to wear a balaclava on the internet do you?

01:21:40 Maxim Alzoba: the same for a tie

01:21:50 Peter Koch: it's the negative of a COVID mask ...

01:22:00 Terry Manderson: Only for you chris... LOL..

01:22:04 Matthias Pfeifer dot.berlin: Maxim: this might be new to some

01:22:14 Volker Greimann: is not the bank where the funds are transferred a better lead?

01:22:20 Tom Dale: Only if you are robbing a dot.bank

01:22:31 Olevie Kouami / Sénégal: Exanple and Example ?

01:22:51 Christian Dawson: Was research ever done on public safety complaints to law enforcement about abuse of unredacted data prior to the implementation of the temp spec? What I mean is that purely public domain registration data was known to be a vector for spam, phishing, doxing, and all kinds of online and physical harassment. Did we do ever word clouds on those past complaints as a point of comparison?

01:22:51 Pelle wecksell Europol sexual abuse against childrenn: I will ask the Ombudsman to go through this chatt after the meeting

01:23:07 Christian Dawson: Was research ever done on public safety complaints to law enforcement about abuse of unredacted data prior to the implementation of the temp spec? What I mean is that purely public domain registration data was known to be a vector for spam, phishing, doxing, and all kinds of online and physical harassment. Did we do ever word clouds on those past complaints as a point of comparison?

01:23:15 Nadira AL Araj - (APRALO): Yes, Exanple @Olevie for vision tricks

01:23:30 Maxim Alzoba: ip addresses are known in less than couple of minutes , and it gives way more info

01:23:31 Olevie Kouami / Sénégal: The delay between the threat and the

01:23:32 Katrin Ohlmer: +1 Christian

01:23:56 Mary Wong (ICANN org): @Jonathan - still no sign of Mark S.

01:24:15 Milton Mueller: It's very early here

01:24:25 Jonathan Robinson (Afilias): Exanple is a homoglyph of Example as far as I can see. It's an example of a homoglyph

01:24:47 Matthias Pfeifer dot.berlin: How could the lack of WHOIS data impact black/blocklists?

01:25:31 Kristof Tuyteleers: Greg clearly only focuses on malicious registrations, not on compromised infrastructure in that last bullet point.

01:25:33 Stephanie Perrin: Were you not up for the previous panel at 3 Milton?

01:25:38 Chris Disspain: as is honoglyph being a homoglyph of homoglyph...

01:25:40 Maxim Alzoba: even after the domain in question deleted - the actual bad content stays on the same place, and actually available via IP. so without hosting companies, ISPs, RIRs there is not a lot to do

01:25:42 Milton Mueller: ha ha ha

01:25:53 Peter Koch: @Jonathan: not quite, PECTOPAH and the same in cyrillic consist of homoglyphs, 'm' vs 'n' is just 'confusingly similar'

01:26:07 margiemilam: Exanple is also a typo-squats - a common way of abusing a famous brand

01:26:19 Mary Wong (ICANN org): Hello all - we appear to be experiencing an issue with the translation app. We are trying to locate the problem to fix. Thank you for your patience.

01:27:05 Maxim Alzoba: the latter lacks evidence - just contact the same kind of cybersecurity companies and ask

01:27:18 Matthias Pfeifer dot.berlin: Oh no Greg...that what they SEE

01:27:24 Roberto: I wonder how exanple has been translated...

01:27:40 Olevie Kouami / Sénégal: @Margie : my understanding too

01:27:40 Lyman Chapin: @Kristof We collected data on both maliciously registered names and compromised sites - they are both covered in the report

01:28:08 Kristof Tuyteleers: I know, but not in that specific statement.

01:28:28 Quoc Pham: Just to point out, redacted public domain registration (accessed via WHOIS or RDAP) still provides delegation data (name servers), registration date (dates, Registrar, etc) and minimal Registrant data (Registrant Organization, Registrant State/Province and Registrant Country) ... much less than previous but still has some data points that are still useful.

01:28:43 Ozan Sahin: Hello all - We have been informed that the problem with the translation applications has been fixed. Thank you for your understanding.

01:28:44 Maxim Alzoba: Rate limiting is against data mining

01:29:09 Maxim Alzoba: and data mining is not what public interest is

01:29:55 Matthias Pfeifer dot.berlin: mhm..gdpr is law that dont care what icann thinks about

01:29:56 Michele Neylon (Blacknight): Reverse whois was NEVER part of whois

01:29:57 Quoc Pham: *public domain registration data

01:30:03 Maxim Alzoba: tracking activities of a person - like what is registered is not in spirit of GDPR

01:30:35 Reg Levy - Tucows: thank you, Quoc

01:31:14 Kristof Tuyteleers: One can always ask to work together instead of trying to suck out all the data from the whois databases and then commercialise that for his own profit.

01:31:20 Olevie Kouami / Sénégal: Wow ! Cool !

01:31:26 Gabriel: @ Michele reverse whois was not a part of WHOIS, true - but it was enabled as a consequence of WHOIS being available, yes? And has disappeared as a viable tool as a consequence of WHOIS redaction. I think that's fair to say, yes?

01:31:56 Reg Levy - Tucows: +1 Kristof

01:32:24 Mary Wong (ICANN org): @Jonathan, looks like a few questions for Greg/Lyman. Want to take them before moving on? (NOTE: still no Mark S).

01:32:41 Milton Mueller: no, we will do presentations and then deal with questions

01:32:50 Milton Mueller: that was agreed

01:32:58 Peter Koch: what are the characteristics of the remaining 40%?

01:33:13 Maxim Alzoba: ICANN is not the place to contact hoster providers, and those are known in seconds (from ip addresses)

01:33:15 Olevie Kouami / Sénégal: Are the registrars selling domain names to sell only ?

01:33:52 Kristof Tuyteleers: @Peter, we have completely different stats ... it depends on the zone

01:34:07 Mary Wong (ICANN org): PANELISTS: Please remember to use "Panelists and Attendees" in the dropdown menu if you wish your comment to be visible to the attendees (and not just panelists/presenters).

01:34:25 Matthias Pfeifer dot.berlin: As a registry, we often do not receive registrant data from registrars.

01:34:26 Maxim Alzoba: not all registrar

01:34:27 Michele Neylon (Blacknight): Olevie?

01:34:39 Maxim Alzoba: not all registries see contact data

01:34:41 Katrin Ohlmer: Registries do not have contact data - it's GDPR time!

01:35:15 Matthias Pfeifer dot.berlin: Well, correct Impressum data on phishing sites could be the solution

01:35:37 Dirk Krischenowski: Many registries have only default/proxy contact data in their database. That helps not much.

01:35:38 Quoc Pham: Depending on the policy of the Registry (if it's thick and allows private registrations) then a Registry may receive "private" registration data

01:35:45 Maxim Alzoba: cybersecurity companies are do not have a special role in GDPR - it is not true

01:36:05 Kristof Tuyteleers: btw, what is a "cybersecurity company"?

01:36:23 Matthias Pfeifer dot.berlin: Quoc: no - its not about policy, because of gdpr they just put dummy data in the handle

01:36:25 Maxim Alzoba: and legal grounds = law , not just e-mail from some third party (may be hackers, pretending to be a cybersecurity company)

01:36:36 Olevie Kouami / Sénégal: Merci Greg

01:37:00 Edmon Chung: Just curious is there data indicating a recognizable increase in phishing due to WHOIS redacting because of GDPR?

01:37:06 Tomslin Samme-Nlar: Implementation team implements policy, not relook at policy

01:37:10 Lori Schulman: @Maxim - legal grounds means criminal and civil acts.

01:37:13 Maxim Alzoba: how can a registrar understand if request is really from a cybersecurity company and they have no bad intents?

01:37:17 Reg Levy - Tucows: +1 Milton

01:37:24 Amr Elsadr: Exactly, Milton!!

01:37:32 Olevie Kouami / Sénégal: Intéressant

01:37:46 Elizabeth Behsudi: <QUESTION> what percentage of phishing reports are remediated (domains suspended) by contracted parties without the need for cybersecurity data requests?

01:37:48 Maxim Alzoba: @Lori, law is a local law, but foreign companies barely have any special role

01:37:57 Jorge Cancio: diversity should be promoted more decidedly in such panels...

01:37:57 Lori Schulman: A third party with a civil interest in enforcement has a perfectly legal need for information.

01:38:04 Rick Lane: Great point Milton. This is why the US Congress needs to step in to protect US citizens from the harms that have been caused by the Whois going dark.

01:38:08 Lori Schulman: And a right.

01:38:20 Mary Wong (ICANN org): Hello again everyone; just a reminder to please use the Q&A pod if you have questions you'd like the panel to address. Thank you.

01:38:23 Reg Levy - Tucows: it would be fascinating to hear from European security researchers

01:38:32 Maxim Alzoba: Q&A pod is dark

01:38:42 Volker Greimann: Lori, if they have a legal right to disclosure, there should not be an issue with receiving that disclosure

01:38:53 Brian King (MarkMonitor): To be fair, the email address one uses in registration data need not be personal data

01:38:56 Reg Levy - Tucows: it really does seem as though the only parties who are concerned by post-GDPR whois restrictions are american

01:38:56 Olevie Kouami / Sénégal: Just

01:39:03 Rick Lane: Q&A pod is dark to protect users privacy... ;-)

01:39:19 Michele Neylon (Blacknight): @Liz - Q+A pod

01:39:22 Lori Schulman: @Maxim - the pod is functioning. Maybe check the bottom of your screen. I can see the questions posted.

01:39:27 Michele Neylon (Blacknight): they can't see the questions in the chat

01:39:54 Maxim Alzoba: we do not see any questions from Q&A - it is the issue

01:40:29 Peter Koch: there are currently 11 questions in the Q&A

01:40:41 Mary Wong (ICANN org): @Maxim, the Q&A pod appears to be functioning for most attendees.

01:41:19 Roberto: Does not work for me either

01:41:29 Stephanie Perrin: Not to mention good spam data

01:42:40 Kristof Tuyteleers: and you have to correlate this data with some of the newG's euhm marketing campaigns

01:42:57 Nadira AL Araj - (APRALO): Also registrants getting unwelcomed business marketing offers

01:42:58 Lauren Kapin: Milton raises an important point about the need for data accuracy.

01:42:59 Carlos Reyes: @Greg and @Lyman, there are several questions in the Q&A pod for you.

01:43:04 Maxim Alzoba: the idea that criminals are entering their true data is weird

01:43:14 Reg Levy - Tucows: +1 Nadira

01:43:23 Kristof Tuyteleers: +1 Maxim

01:43:26 Rick Lane: +1@Laureen

01:43:27 Stephanie Perrin: Mazim, do you have the balloon at the top set to "my questions" or all questions?

01:43:42 Owen Smigelski (Namecheap): +1 Theo

01:43:53 hadia Elminiawi: The question is - regardless of the numbers of the Phishing and malware actions - how do we deal with those harmful, criminalized actions effectively and efficiently in the absence of an efficient registration data disclosure system

01:44:26 Matthias Pfeifer dot.berlin: Hadia: call the registrar with valid data and report it

01:44:27 Laureen Kapin: @Theo -- perhaps that points to the need for improved validation procedures?

01:44:29 Reg Levy - Tucows: +1 Hadia

01:44:35 Michele Neylon (Blacknight): Most of the phishing issues we see are with the hosting providers - the domain is irrelevant really

01:44:45 Matthias Pfeifer dot.berlin: thx Milton

01:44:55 Rick Lane: @Milton "We have to comply with the law." Which is again why the US Congress needs to fix the problem

01:45:15 Rick Lane: created by the GDPR

01:45:31 Milton Mueller: so you want to fragment DNS by legal jurisdiction?

01:45:34 Maxim Alzoba: why not requesting ISPs or hosting companies to suppress the actual damaging content?

01:45:53 Rick Lane: It is already fragmented because of the gDPR

01:46:01 Matthias Pfeifer dot.berlin: lol

01:46:07 Maxim Alzoba: it will create clusters of country-nets

01:46:10 Mary Wong (ICANN org): @Greg @Lyman: there are some specific questions for you in the Q&A pod.

01:46:13 Michele Neylon (Blacknight): Rick Lane - we're an Irish company so you can pass law in your Congress as much as you want and we will ignore you

01:46:24 Rick Lane: The GDPR is why we are having this conversation

01:46:33 Michele Neylon (Blacknight): Unless of course your goal is to fragment the internet

01:46:39 Roberto: @Rick - from Milton's data it seems that the problem has not been created by GDPR

01:46:49 Matthias Pfeifer dot.berlin: Rick: No, we have this discussion because of fraud

01:47:19 Rick Lane: I live in the US. If Ireland does not want to protect its citizens from harm that is their decision. Just like the GDPR

01:47:36 Michele Neylon (Blacknight): The internet is global

01:47:45 Matthias M. Hudobnik: @rick it is not about fixing this bis the US. GDPR has a data subject-centric way of determining applicability of the law!

01:47:46 Rick Lane: But countries have borders

01:47:55 Michele Neylon (Blacknight): *yawn*

01:48:11 Amr Elsadr: @Rick: The purpose of GDPR is to protect the privacy/data protection rights of the EU's citizens.

01:48:21 Rick Lane: We can not let the GDPR be the "law" of the world

01:48:30 Matthias Pfeifer dot.berlin: why not?

01:48:31 Kristof Tuyteleers: @rick so please only allow you US hackers hack into US systems located in the US ...

01:48:33 Amr Elsadr: @Rick: It was a legal right before GDPR was a thing.

01:48:40 Jonathan Zuck: Thanks @Mark, we'll go to you next.

01:48:49 Rick Lane: Not here in the US

01:49:01 Roberto: @Rick - we cannot have US law upon the world either, though

01:49:28 Michele Neylon (Blacknight): so you're actually proud that you don't respect your citizens' rights to privacy? Wow

01:49:30 Mary Wong (ICANN org): @Jonathan - Mark is here.

01:49:39 Maxim Alzoba: fi the law is too limiting roles of other countries, then the fragmentation will happen in months

01:49:41 Amr Elsadr: @Rick: So maybe lobby legislators in the US to draft laws that protect the privacy of US citizens too? Are US citizens not worthy of personal privacy?

01:49:42 Michele Neylon (Blacknight): Impressive in a sort of smack my head against a wall stupid sort of way

01:49:50 Elizabeth Behsudi: This issue isn't whether any particular law is deemed to be extra-territorial. US companies who are not compliant with GDPR will not receive data transfers from European businesses

01:50:14 hadia Elminiawi: @Roberto malware and phishing have always been there, but the problem now is that we do not have an efficient system for data disclosure which can help mitigate theses harmful actions

01:50:24 Rick Lane: Each country has to make decisions about how to "protect" their citizens

01:51:08 Amr Elsadr: Yup..., and some countries do a better job than others.

01:51:37 Matthias Pfeifer dot.berlin: fact is: cybercriminals give a sh** on law/borders/policy erywehere. We need to improve processes to take down malicious content or to make it harder to host and install it. policy/law is just a small part in that game...

01:52:08 Rick Lane: How many companies in the EU have been held accountable under GDPR? I will put our US FTC enforcement actions against any other privacy regime

01:52:24 Matthias Pfeifer dot.berlin: doing updates on old cms or operating systems will improve security more that a law..

01:52:34 Luc Seufer: Held accountable for not abiding by GDPR?

01:52:40 Maxim Alzoba: mitigation can be done even without knowing the PI , you have the contents and IP addresses - it is enough

01:52:41 hadia Elminiawi: We are looking for a system that certainly complies with the law but allows for the data to provided for legitimate interests and lawful basis in a timely and efficient manner

01:52:49 Roberto: @Hadia - I fully agree - I only have an issue with the wording used - GDPR might have eliminated the easy solution that was to ignore privacy, but the fact that a balance between security and privacy has not been found in years cannot be imputed to GDPR, but to some stubborn positions

01:53:32 Maxim Alzoba: the assumption that self called cybersecurity companies have a special legal role is not based on law

01:53:54 Matthias Pfeifer dot.berlin: :)

01:54:03 Rick Lane: I find it interesting that this is about a "world" Internet, but their privacy regime is better so it must be the "worlds" privacy regime. You cannot have it both ways

01:54:39 Maxim Alzoba: we do not know, how many bad actors pretend to be cybersecurity researchers, and if the special role is granted , such numbers will grow

01:54:45 Jeffrey Neuman: All - I put this question in the Q&A Pod - "I want to ask the same question I raised during yesterday's plenary in line with Monday's public session discussing ICANN meetings in general. What is the purpose/goal of this Plenary? How does this Plenary advance the work of ICANN? And, What do the panelists believe are the next steps?"

01:54:58 Matthias M. Hudobnik: @ rick it is very clear if you are a data controller and processing (offering goods or services or monitoring behaviour) personal data of a data subject in the eu you are bound by the GDPR even if you reside in the US!

01:55:10 Milton Mueller: no, you cannot have it both ways. We need globalized privacy protection just as we need a global DNS root and globalized policy for DNS, that's why we have ICANN.

01:55:32 Laureen Kapin: @ Owen, please discuss the number of registries/registrars who responded to the survey discussed? My understanding based on the webinar was that it was a small number.

01:55:38 Jonathan Zuck: +1 Ashley

01:55:54 Michele Neylon (Blacknight): @Laureen - maybe put that in the Q A pod - he might not see it here

01:56:22 Rick Lane: ICANN is not a government which is why this issue cannot be solved by ICANN. That was basically Marby's point.

01:56:48 Milton Mueller: now who would that big requester be

01:57:08 Matthias Pfeifer dot.berlin: the issue could never be solved..we just can make it better

01:57:12 Laureen Kapin: Agreed Ashley --- this is useful info -- I just think it needs to put in context.

01:57:14 Goran Marby: Rick: when did I make that point?

01:57:42 Goran Marby: Because that seems to be taken a little bit of context.

01:57:53 Milton Mueller: ICANN is not a "government" obviously but it does govern the DNS

01:57:58 Milton Mueller: via contract law

01:58:21 Owen Smigelski (Namecheap): Practical Insights from Contracted Parties (presentation):

<https://gnso.icann.org/sites/default/files/policy/2020/presentation/presentation-Practical%20Insights-22sept20-en.pdf>

01:58:27 Volker Greimann: maybe the US could just adopt the GDPR or some form of it. it would help data transfer and equivalence issues.

01:58:30 Cheryl Langdon-Orr: Hi @Mark :-)

01:58:32 Rick Lane: The US cannot allow ICANN to put our citizens in harms way.

01:58:41 Owen Smigelski (Namecheap): Zoom recording:

<https://icann.zoom.us/rec/share/Xocs4MStN4CGoDJwBp4B5Mv3axUYQJEI0nMzG3SN6SsN69IR6G3Abmd0VYOpPXM.Ma.GezcRh6gJv3BtoGa?startTime=1600783345000>

01:58:41 Laureen Kapin: @ Marc SV -- we've all been there!

01:58:49 Mark Svancarek: <https://www.microsoft.com/en-us/download/confirmation.aspx?id=101738>

01:59:00 Kristof Tuyteleers: is that a phishing link?

01:59:06 Maxim Alzoba: provision of the PI online harms citizens , just another way

01:59:51 Ozan Sahin: Hi Bruce. This is the only slide for Mark.

02:02:26 Luc Seufer: Can someone bring Mark a coffee?

02:02:36 Michele Neylon (Blacknight): Um

02:03:01 Rick Lane: ICANN governs the DNS by contracts it does not enforce. Nor do the contracted parties. In addition, we as Internet users have no mechanisms or standing to enforce those contracts.

02:03:24 Michele Neylon (Blacknight): Coffee break time maybe?

02:03:32 Luc Seufer: Q&A!

02:03:55 Matthias Pfeifer dot.berlin: Rick: your second point is simply not true

02:04:07 Mary Wong (ICANN org): As our moderator requested, you can find the link to the webinar recording and slides from the Contracted Parties' webinar from last month, about "Practical Insights on Data Disclosure": <https://www.rysg.info/webinars-and-presentations>

02:04:17 Rick Lane: Therefore, we are at the mercy of contracted parties who have millions of dollars at stake. This is the flaw of the multi-stakeholder process "fails" in this area.

02:04:56 Milton Mueller: and you as IPC have billions of dollars invested in free access to private data, Mr Lane

02:05:05 Rick Lane: This is the flaw of the multi-stakeholder process and why the EPDP "fails" in this area.

02:05:37 Michele Neylon (Blacknight): With a phish you want the site down quickly

02:05:56 Michele Neylon (Blacknight): I don't see why you'd be asking for domain registration data FIRST

02:06:12 Owen Smigelski (Namecheap): @Rick- reaching agreement among various and disparate positions is... what the MSM is all about. Just because your side does not get 100% of what it thinks is "correct" does not mean it's a failure. It means it's working, and stop claiming it's not.

02:06:34 Milton Mueller: I'd like to address it also, Jonathan

02:06:44 Rick Lane: Whois is not "private" data. Just like land records in the US.

02:06:45 Matthias Pfeifer dot.berlin: Michele: we still have the need for translation tech <> lawyer

02:06:46 Jorge Cancio: who is speaking?

02:06:55 Michele Neylon (Blacknight): Jorge - Greg Aaron

02:06:58 Jonathan Zuck: Greg Aaron

02:07:07 Jorge Cancio: thx!

02:07:21 Gabriel: and yet the emoji was perfect ;)

02:07:27 Amr Elsadr: @Rick: What would the scenario have been, in your opinion, where the EPDP would have "succeeded"? What could the EPDP have done better for SSAD users, while still comply with applicable law?

02:07:39 Benedict Addis: @Michele different roles. Maybe takedown isn't my job, but I need to collate clues for an investigation into a phishing gang

02:08:05 Luc Seufer: So less domains are used for illicit purpose. (yeay registrars)

02:08:30 Michele Neylon (Blacknight): Benedict - like I get you might like to have the data but in a phish the first thing you want is to get the site down

02:08:34 Rick Lane: @Arm The problem is a "law" that is harming US citizens

02:08:48 Rick Lane: or at least its interpretation

02:08:49 Kristof Tuyteleers: @Luc Less domains, but more abuse cases per misused domain

02:09:45 Matthias Pfeifer dot.berlin: well..developing malware is going to be harder that years ago. Thats also one point why we see another landscape regarding malware..

02:10:01 Luc Seufer: Which shows that hosting providers need to take action like registrars do

02:10:12 Alan Woods (Donuts): apologies - sent this only to the panellists - Perhaps Mark is referring to the ICO. "Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing has to be absolutely essential. However, it must be more than just useful, and more than just standard practice. It must be a targeted and proportionate way of achieving a specific purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means, or by processing less data." As a data controller, I completely agree with this. I would urge all to listen to the CPH webinar , specifically Beth Bacon's section relating to the types of requests, the data we need to establish the realistic necessity in a request - again focussing on our legal obligations to the data subject. Disclosure is still absolutely possible and is a priority, but we must ensure due process is followed.

02:10:50 Amr Elsadr: @AlanW: Thank you!!

02:11:05 Sarah Wyld: +1 Luc, +1 AlanW

02:11:12 Brian King (MarkMonitor): @AlanW thank you

02:12:08 Maxim Alzoba: all the discussions here are about phishing only, why not calling the panel accordingly?

02:12:09 Kristof Tuyteleers: @Greg I have examples where hacked mailboxes were used

02:12:29 Brian King (MarkMonitor): +1 to the data still being valuable. Criminals do tend to provide incorrect data consistently, with patterns and trends that can help 'connect the dots'

02:12:34 Maxim Alzoba: taking down the domain does not take down the content

02:12:41 Ozan Sahin: Panelists - Please remember to say your name before responding to a question.

02:13:35 Samaneh Tajalizadehkhoob: Every set of reputation list (RBL) provide partial view. Given that research on RBL comparison already shows there is very little overlap across RBLs, no matter what tool or what reserach paper, what is reported as "trend" is always from the perspective of that specific dataset, and therefore is partial. It could be DAAR or other tools and research. What we should be careful about is the correct interpretation of the data and terminology around it, that is: What we see is not a universal trend, is a trend based on the data we use as input.

02:13:40 Samaneh Tajalizadehkhoob: Every set of reputation list (RBL) provide partial view. Given that research on RBL comparison already shows there is very little overlap across RBLs, no matter what tool or what reserach paper, what is reported as "trend" is always from the perspective of that specific dataset, and therefore is partial. It could be DAAR or other tools and research. What we should be careful about is the correct interpretation of the data and terminology around it, that is: What we see is not a universal trend, is a trend based on the data we use as input.

02:13:40 Matthias Pfeifer dot.berlin: Maxim: the most crowd-phising attacks are not so fancy to deal with domains that are gone

02:14:06 Jorge Cancio: if anyone is in the mood of reading a short comic strip on phishing: visit <https://www.websters.swiss/en/s1/5>

02:15:03 Maxim Alzoba: criminals are aware of the dictionaries, and not necessary use machine like names

02:15:07 michaelgraham: @Milton — The inability to identify phisher block-registrants via using WHOIS for Reverse-WHOIS has become a real and expensive problem.

02:15:26 Michele Neylon (Blacknight): Reverse whois was NEVER part of whois

02:15:39 Amr Elsadr: @Michael: Reverse Whois?!

02:15:44 Maxim Alzoba: reverse-whois is not about ICANN, it is some third parties doing something

02:15:49 Owen Smigelski (Namecheap): +1 Michele

02:15:51 Michele Neylon (Blacknight): +1 Maxim

02:15:57 Amr Elsadr: @Maxim: +1

02:16:25 Roberto: +1 Maxim & Michele

02:16:43 michaelgraham: @Michele — Correct, but the completeness of available WHOIS information enabled reverse WHOIS. Whether it is PART of WHOIS is not really the issue.

02:16:46 Maxim Alzoba: if we think that the valid data of criminals is in whois ... we are trying to catch retarded criminals only

02:16:59 Milton Mueller: Again, no real data

02:17:12 Jorge Cancio: it seems as if we are still far from really having a conversation... sounds more like different discourses in parallel... 🙄

02:17:14 Matthias Pfeifer dot.berlin: Michael: thats not allowed due to gdpr

02:17:29 michaelgraham: @Maxim — You might be surprised. It might be false information — but it's more often than not consistent false information.

02:17:40 Maxim Alzoba: data mining for PI by such third parties is a violation of those persons citizens rights

02:17:43 Milton Mueller: Jorge, that's been going on for 15 years

02:17:55 Lori Schulman: @Maxim, even inaccurate information can provide patterns of information that can be correlated to particular bad actors. Also, kindly refrain from using the word "retarded".

02:18:07 michaelgraham: @Jorge — Agree. Frustratingly similar to modern political discourse.

02:18:18 Luc Seufer: For what it worth, the majority of phishing domain names registered only for this purpose (not hacked websites) are registered with stolen payment methods. We are not making any money on those and have to pay chargeback fees.

02:18:19 Jorge Cancio: Milton... that's not a very efficient use of time, right?

02:18:20 michaelgraham: +1 Lori

02:18:25 Amr Elsadr: @Michael: The service you're referring to is provided in stark conflict with the law. Up to all of us to come up with legal alternatives.

02:18:39 Milton Mueller: I would like very much to get to your and Jeff Neuman's question ;-)

02:18:43 Maxim Alzoba: @Lori, sorry , I am not a native speaker, I meant not well thinking

02:19:05 Jorge Cancio: @Milton, indeed

02:19:09 Mohit Batra: Domain Generation Algorithms have also their role to play in attackers' toolkit. ICANN Org should develop best practices and provisions in its agreements with Registries and Registrars that make it harder for attackers to use DGA's for malicious purposes.

02:19:19 Lori Schulman: @Maxim - apology accepted. No worries.

02:19:32 michaelgraham: @Amr — Creates an interesting question of law protecting wrongdoing.

02:19:42 Lori Schulman: +1 to Mohit

02:19:53 Rick Lane: +1 Lori on both points

02:20:22 michaelgraham: @Amr— Agree that approach and solution has to be within the law — especially within the intent of the law.

02:20:43 Maxim Alzoba: following hosters and AS (ip addresses) will give way more information way faster (and available in seconds)

02:20:55 Luc Seufer: How would you know what a domain name will be used for and how the string of characters have been selected?

02:21:05 Matthias Pfeifer dot.berlin: Maxim++

02:21:19 Alex Deacon: @maxim - investigators reach out to all service providers involved.

02:21:50 Amr Elsadr: @Michael: Not exactly the way I see it re: law protecting wrongdoing. The law should not protect the rights of some at the expense of the rights

of others. There must be a workable solution, and I suspect we'll get there soon enough. SSAD is just the first step, and not a final solution.

02:21:51 Maxim Alzoba: @Alex, we do not feel like that, at least from the usual sets of materials presented

02:22:16 Peter Koch: treating prevention, mitigation, and investigation separately might actually improve focus

02:22:17 michaelgraham: @Amr — Let's hope.

02:22:34 Susan.Payne Valideus/ComLaude: @Owen - that is a very simplistic assessment of the balancing test to suggest that because you can bring a UDRP you do not need the data. For example, an element of the UDRP includes demonstrating elements like a pattern of conduct. How would you suggest that is done without access to the relevant information. It's also a defence in a UDRP for their to be a legitimate right or interest to the name - how does the brand owner know that without the info?

02:22:35 Kristof Tuyteleers: +1 for Peter

02:22:42 Craig Schwartz (.BANK): @Brian B - please post link in chat that you just did in Q&A as it cannot be copied.

02:22:52 michaelgraham: Can i turn on mic?

02:24:13 Rick Lane: All multi-national businesses have to figure out have to comply with conflicting laws. That is the cost of doing business as a multi-national

02:24:37 Maxim Alzoba: where there attempts to reach e-mail providers ? even marking phishing mails as spam and putting in the spam box would help a lot

02:25:15 Amr Elsadr: @Rick: Finally, something we can agree on. :-)

02:25:40 Volker Greimann: hence an imprint on the website and signatures in an email should be required for commercial use.

02:26:02 Brian King (MarkMonitor): While RDS data used to be validated to obtain a SSL/TLS certificate (OV certs), post-GDPR domain-validated (DV) certs have become far more popular. We trained consumers to trust sites with an SSL, however now 77+% of phishing attacks are hosted on HTTPS, up from 35% pre-GDPR.

02:26:02 Amr Elsadr: @Milton: +1

02:26:14 Maxim Alzoba: there is no question of balance - we have to comply with the law

02:26:17 Brian King (MarkMonitor): (according to APWG)
https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

02:26:19 Rick Lane: +1 Amr

02:26:26 Michele Neylon (Blacknight): Brian - the browsers are almost hiding the SSL these days

02:26:36 michaelgraham: @Milton — and Hence Privacy and Proxy

02:27:13 Brian King (MarkMonitor): The difference in opinion here is who the victim is

02:27:29 Brian King (MarkMonitor): The cybercriminal being investigated is the cost causer.

02:27:45 Brian Beckham (WIPO): The link from my Q in the Q&A pod:
https://edps.europa.eu/sites/edp/files/publication/19-02-25_proportionality_guidelines_en.pdf

02:27:45 Russ Pangborn: +1 Brian K

02:27:51 Roberto: I am not always agreeing with @Milton, but this time I am completely

02:27:57 Craig Schwartz (.BANK): Thx BB

02:28:12 Matthias M. Hudobnik: + 1 Milton!

02:28:20 Maxim Alzoba: how does a contracted party distinguish the bad actors from real cybersecurity companies? (from afar)

02:28:38 Peter Koch: @Brian @Michele the presence of TLS has never been a positive signal - just the absence is a negative

02:28:53 Maxim Alzoba: models are per jurisdiction

02:28:57 Matthias Pfeifer dot.berlin: maxim: the bad guys wearing black hats

02:29:12 Maxim Alzoba: the same for Law Enforcement

02:29:16 Rick Lane: Is the .dk requirement of having an open, accurate and accessible whois a violation of GDPR?

02:29:28 michaelgraham: @Milton — I would not limit the consideration of “cost” to financial cost — there is a REAL cost to user confidence and effective communication. Tracking just the few complaints filed with Attorney Generals and FTC reveal some of the user cost.

02:29:28 Kristof Tuyteleers: @Brian @Michele @Peter and pushed by search engines and browser vendors, not by GDPR

02:29:32 Brian Beckham (WIPO): link to ICO guidance from question in Q&A pod: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/>

02:29:51 Amr Elsadr: Simply owning a trademark isn't grounds to disclosing registration data. There needs to be a little more to it than that.

02:29:52 Maxim Alzoba: only the relevant DPA can say if .dk is following GDPR or not

02:29:53 Milton Mueller: Mike Graham can you quantify that cost?

02:30:41 Stephanie Perrin: Better add the cost to DPAS of handling registrant complaints also.

02:30:46 Ozan Sahin: @Jonathan - we have 3 minutes left.

02:31:18 Rick Lane: And the DPA has not said that it is a violation of GDPR. But the stats on harm mitigation from .dk's open whois is stunning.

02:31:35 Maxim Alzoba: are there any safeguards from cybersecurity companies leaking PI out?

02:31:45 Volker Greimann: laureen, but it does protect the personal information of natural entities included in the data of the legal entities...

02:32:00 Milton Mueller: Yes, Laureen an impressum law in the US would be a great thing. Make all legal persons publish their contact data

02:32:06 Maxim Alzoba: @Rick, it is not relevant for other parties, DPA investigate only one particular case

02:32:14 Katrin Ohlmer: +1 Milton

02:32:26 Volker Greimann: laureen, in those cases it is made publicly available as a legal requirement

02:32:36 Nick.Wood: I believe there is a "Domain Name LAW" in Denmark. This is the platform for the efforts of .dk

02:32:51 michaelgraham: @Milton — That is part of the difficulty, is it not: How do you quantify damage to consumers? I can say that one fraudulent scheme that used the DNS resulted in cost to consumers that we learned of of several hundreds of thousands of dollars. But we can no more quantify user financial, trust, and other cost than we can the cost of revealing their personal information.

02:32:59 Cheryl Langdon-Orr: Thanks everyone this has been most useful

02:33:05 Volker Greimann: that is one such wxample, Nick. solces a lot of issues.

02:33:07 Maxim Alzoba: we can not use Denmark laws outside of that country

02:33:08 Mark Svancarek: @Nick, the Domain Name Act provides the basis for open WHOIS in .DK

02:33:14 Volker Greimann: solves

02:33:16 Louie Lee: Thank you!

02:33:19 Rick Lane: Thanks Jonathan

02:33:19 Louie Lee: Thanks everyone.

02:33:21 Alan Woods (Donuts): @brian - re your question - the fact of the matter is that such disclosure decisions will consider that as a factor - but it would help if proper requests are made to help us establish that. Also your point turns on an allegation of an infringement - and not all allegations are created equally - and hence the human review is deemed not only necessary - but based on the quality of requests I have seen, especially from some very well informed and well funded third parties, it is just common sense and prudent.

02:33:25 Nadira AL Araj - (APRALO): Indeed it is good interactive session.
Thanks Jonathan Zuck for moderating this session

02:33:27 Amr Elsadr: Thanks all. Bye.

02:33:29 Owen Smigelski (Namecheap): 3am for me too!

02:33:33 hadia Elminiawi: Thank you all - bye

02:33:33 Maxim Alzoba: thanks all

02:33:38 Herb Waye: Great respectful discussion

02:33:40 michaelgraham: @Jonathan — Thanks.

02:33:42 yaovi.atohoun: Thanks ans bye

02:33:43 Matthew Shears: Thanks all!

02:33:44 Cheryl Langdon-Orr: bye for now